Claims:

1. (Currently amended) A method comprising:

~~selectively hashing a first data string;~~

generating first and second random values to allow a signature-generating process to encrypt and decrypt a data block;

digitally signing a ~~second data~~ first string, wherein the first string includes the first random value; and

generating an encryption key for encrypting the data block by hashing a combination of ~~based on~~ the digitally signed ~~second data~~ first string and the second ~~a third data string~~ random value.

2. (Currently amended) The method as recited in Claim 1, further comprising:

selectively encrypting the data block using the encryption key.

3. (Currently amended) The method as recited in Claim 2, ~~wherein~~ further comprising:

generating a third random value;

obtaining a hash of the third random value; and

including the third random value and the hash of the third random value in the data block to be encrypted ~~the data includes the hash of the first data string~~.

4. (Currently amended) The method as recited in Claim ~~2~~ 3, ~~wherein~~ further comprising decrypting the data block using a decryption key to obtain a decrypted data block, wherein the decrypted data block includes a decrypted third random value and a decrypted hash of the third random value;

~~the data includes~~ obtaining a hash of the decrypted ~~first~~ third random value ~~data string;~~ and

verifying the decryption key by comparing the hash of the decrypted third random value with the decrypted hash of the third random value.

5. (Currently amended) The method as recited in ~~Claim 4~~ Claim 2, further comprising storing the encrypted data block, the ~~second~~ first random value ~~data string~~ and the ~~third~~ second random value ~~data string~~.

6. (Currently amended) The method as recited in Claim 5, ~~wherein~~ further comprising:

accessing the stored encrypted data block, the stored ~~second~~ first random value ~~data string~~ and the stored ~~third~~ second random value; ~~data string are each stored in memory~~

digitally signing a second string, wherein the second string includes the stored first random value; and

generating a decryption key by hashing a combination of the digitally signed second string and the stored second random value.

7. (Currently amended) The method as recited in Claim 5, wherein the encrypted data block, the ~~second~~ first random value ~~data string~~ and the ~~third~~ second random value ~~data string~~ are each stored on a storage medium.

8. (Canceled)

9. (Currently amended) The method as recited in ~~Claim 8~~ Claim 1, wherein generating the encryption key further includes cryptographically hashing the digitally signed ~~second data~~ first string concatenated with the ~~third~~ second random value ~~data string~~.

10. (Currently amended) The method as recited in ~~Claim 8~~ Claim 1, wherein generating the encryption key further includes cryptographically hashing the ~~third~~ second random value ~~data string~~ concatenated with the digitally signed ~~second data~~ first string.

11. (Canceled)

12. (Currently amended) The method as recited in Claim 1, wherein a first device generates the first random value, ~~data string,~~ the second random value, and ~~data string and the third data string are each generated by a first device that is configured to selectively hash the first data string and generate~~ the encryption key.

13. (Currently amended) The method as recited in Claim 1, wherein a second device digitally signs the ~~second data~~ first string.

14. (Currently amended) The method as recited in Claim 13, wherein the second device comprises ~~includes~~ a signature-generating device.

15. (Currently amended) The method as recited in Claim 14, wherein the signature-generating device ~~is~~ comprises a smart card.

16. (Currently amended) A computer-readable medium having computer-executable instructions for performing steps comprising:

~~selectively hashing a first data string;~~

generating first and second random values to allow a signature-generating process to participate in encrypting and decrypting a data block;

digitally signing a ~~second data~~ string that includes the first random value; and

generating an encryption key based on the digitally signed ~~second data~~ string and ~~a third~~ the second random value ~~data string~~.

17. (Currently amended) The computer-readable medium as recited in Claim 16, further comprising computer-executable instructions for:

selectively encrypting the data block using the encryption key.

18. (Currently amended) The computer-readable medium as recited in Claim 17, ~~wherein~~ further comprising instructions for:

generating a third random value;

hashing the third random value; and

including the third random value and the hash of the third random value in the data block ~~includes the hash of the first data string~~.

19. (Currently amended) The computer-readable medium as recited in Claim ~~17~~ 18, further comprising instructions for:

~~wherein the data includes the first data string~~ decrypting the data block using a decryption key to obtain a decrypted data block, wherein the decrypted data block includes a decrypted third random value and a decrypted hash of the third random value;

obtaining a hash of the decrypted third random value; and

verifying the decryption key by comparing the hash of the decrypted third random value with the decrypted hash of the third random value.

20. (Currently amended) The computer-readable medium as recited in Claim ~~19~~ 17, further comprising computer-executable instructions for:

storing the encrypted data block, the ~~second data string~~ first random value and the second random value ~~third data string~~.

21. (Currently amended) The computer-readable medium as recited in Claim 20, ~~wherein the~~ further comprising computer-executable instructions for:

accessing the stored encrypted data block, the stored ~~second~~ first random value ~~data string~~ and the stored ~~third~~ second random value; ~~data string are each stored in memory~~

digitally signing a second string, wherein the second string includes the stored first random value; and

generating a decryption key by hashing a combination of the digitally signed second string and the stored second random value.

22. (Currently amended) The computer-readable medium as recited in Claim 20, wherein the encrypted data block, the ~~second data string~~ first random value and the ~~third~~ second random value ~~data string~~ are each stored on a storage medium.

23. (Canceled)

24. (Currently amended) The computer-readable medium as recited in Claim ~~23~~ 16, wherein generating the encryption key further includes cryptographically hashing the digitally signed ~~second data~~ string concatenated with the second random value ~~third data string~~.

25. (Currently amended) The computer-readable medium as recited in Claim ~~23~~ 16, wherein generating the encryption key further includes cryptographically hashing the ~~third data string~~ second random value concatenated with the digitally signed ~~second data~~ string.

26. (Canceled)

27. (Currently amended) The computer-readable medium as recited in Claim 16, wherein the first random value and ~~data string,~~ the second random value ~~data string and the third data string~~ are each generated by a first device that is configured to ~~selectively hash the first data string and~~ generate the encryption key.

28. (Currently amended) The computer-readable medium as recited in Claim 16, wherein a second device digitally signs the ~~second data~~ string.

29. (Original) The computer-readable medium as recited in Claim 28, wherein the second device includes a signature-generating device.

30. (Original) The computer-readable medium as recited in Claim 29, wherein the signature-generating device is a smart card.

31. (Currently amended) An arrangement comprising:

first logic configured to selectively hash a first data string, wherein the first data string and the hash of the first data string are to be included in a data block to be encrypted by a signature-generating process;

second logic operatively coupled to the first logic and configured to digitally sign a second data string; and

wherein the first logic is further configured to generate an encryption key based on a combination of the digitally signed second data string and a third data string.

32. (Currently amended) The arrangement as recited in Claim 31, wherein the first logic is further configured to selectively encrypt the data block using the encryption key.

33. (Canceled)

34. (Canceled)

35. (Currently amended) The arrangement as recited in Claim ~~34~~ 32, wherein the first logic is further configured to store the encrypted data, the second data string and the third data string.

36. (Currently amended) The arrangement as recited in Claim 35, further including memory operatively coupled to the first logic, ~~and~~ wherein the first logic stores the encrypted data, the second data string and the third data string ~~are~~ in the memory.

37. (Original) The arrangement as recited in Claim 35, further including a data storage device having at least one storage medium, the data storage device being operatively coupled to the first logic, and wherein the first logic provides the encrypted data, the second data string and the third data string to the storage device for storage on a storage medium.

38. (Canceled)

39. (Currently amended) The arrangement as recited in Claim ~~38~~ 31, wherein the first logic is further configured to cryptographically hash the digitally signed second data string concatenated with the third data string.

40. (Currently amended) The arrangement as recited in Claim ~~38~~ 31, wherein the first logic is further configured to cryptographically hash the third data string concatenated with the digitally signed second data string.

41. (Currently Amended) The arrangement as recited in Claim 31, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a ~~substantially~~ randomly generated data string.

42. (Original) The arrangement as recited in Claim 31, wherein the first data string, the second data string and the third data string are each generated by the first logic.

43. (Original) The arrangement as recited in Claim 31, wherein the second logic is provided within a smart card.

44. (Currently amended) A method comprising:

~~accessing~~ generating first, second, and third ~~a plurality of stored~~ data strings;

digitally signing ~~a~~ the second data string; and

generating an encryption key for encrypting a data block based on the digitally signed second data string and ~~a~~ the third data string;

encrypting the data block using the encryption key; and

storing the encrypted data block, the second data string, and the third data string.

45. (Currently amended) The method as recited in Claim 44, further comprising:

accessing the stored encrypted data block, the stored second data string, and the stored third data string;

digitally signing the second data string accessed from storage;

generating a decryption key based on the digitally signed second data string and the third data string accessed from storage; and

decrypting the encrypted data block using the ~~en~~decryption key.

46. (Currently amended) The method as recited in Claim 45, wherein the resulting decrypted data block includes the first data string.

47. (Currently amended) The method as recited in Claim 46, wherein the resulting decrypted data block includes a hash of the first data string.

48. (Currently amended) The method as recited in Claim 45, wherein the accessing ~~the plurality of stored data strings and accessing the encrypted data~~ further includes reading a memory.

49. (Currently amended) The method as recited in Claim 45, wherein the accessing ~~the plurality of stored data strings and accessing the encrypted data~~ further includes reading data from at least one storage medium.

50. (Canceled)

51. (Currently amended) The method as recited in Claim ~~50~~ 44, wherein generating the encryption key further includes cryptographically hashing the digitally signed second data string concatenated with the third data string.

52. (Currently amended) The method as recited in Claim ~~50~~ 44, wherein generating the encryption key further includes cryptographically hashing the third data string concatenated with the digitally signed second data string.

53. (Currently Amended) The method as recited in Claim 44, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a ~~substantially~~ randomly generated data string.

54. (Original) The method as recited in Claim 44, wherein the first data string, the third data string, and the encrypted data are each accessed by a first device that is configured to selectively hash the first data string and generate the encryption key.

55. (Original) The method as recited in Claim 44, wherein a second device digitally signs the second data string.

56. (Original) The method as recited in Claim 55, wherein the second device includes a signature-generating device.

57. (Original) The method as recited in Claim 56, wherein the signature-generating device is a smart card.

58. (Currently amended) A computer-readable medium having computer-executable instructions for performing steps comprising:

accessing from storage first, second, and third ~~a plurality of stored~~ data strings;

digitally signing ~~a~~ the second data string; ~~and~~

generating an encryption key based on the digitally signed second data string and ~~a~~ the third data string; and

encrypting a data block using the encryption key.

59. (Currently amended) The computer-readable medium as recited in Claim 58, further comprising computer-readable medium having computer-executable instructions for:

accessing the encrypted data block; and

decrypting the encrypted data block using the encryption key.

60. (Currently amended) The computer-readable medium as recited in Claim 59, wherein the resulting decrypted data block includes ~~a~~ the first data string.

61. (Currently amended) The computer-readable medium as recited in Claim 60, wherein the resulting decrypted data block includes a hash of the first data string.

62. (Currently amended) The computer-readable medium as recited in Claim 59, wherein the accessing ~~the plurality of stored data strings and accessing the encrypted data~~ further includes reading a memory.

63. (Currently amended) The computer-readable medium as recited in Claim 59, wherein the accessing ~~the plurality of stored data strings and accessing the encrypted data further~~ includes reading data from at least one storage medium.

64. (Canceled)

65. (Currently amended) The computer-readable medium as recited in Claim ~~64~~ 58, wherein generating the encryption key further includes cryptographically hashing the digitally signed second data string concatenated with the third data string.

66. (Currently amended) The computer-readable medium as recited in Claim ~~64~~ 58, wherein generating the encryption key further includes cryptographically hashing the third data string concatenated with the digitally signed second data string.

67. (Currently Amended) The computer-readable medium as recited in Claim 58, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a ~~substantially~~ randomly generated data string.

68. (Original) The computer-readable medium as recited in Claim 58, wherein the first data string, the third data string, and the encrypted data are each accessed by a first device that is configured to selectively hash the first data string and generate the encryption key.

69. (Original) The computer-readable medium as recited in Claim 58, wherein a second device digitally signs the second data string.

70. (Currently amended) The computer-readable medium as recited in Claim 69, wherein the second device ~~includes~~ performs a signature-generating ~~device~~ process.

71. (Currently amended) The computer-readable medium as recited in Claim 70, wherein a smart card performs the signature-generating ~~device~~ process ~~is a smart card~~.

72. (Currently amended) A ~~n arrangement~~ system comprising:

a data block to be encrypted by an encryption key;

a first device capable of generating the encryption key;

a second device capable of digitally signing a string;

first logic associated with the first device ~~configured~~ to generate first, second, and third ~~access a plurality of stored~~ data strings;

second logic associated with the second device ~~cooperatively coupled to the first logic and configured~~ to digitally sign ~~a~~ the second data string; and

~~wherein~~ at least a part of the first logic ~~is~~ further configured to generate ~~an~~ the encryption key based on the digitally signed second data string and ~~a~~ the third data string.

73. (Currently amended) The ~~arrangement~~ system as recited in Claim 72, wherein the first logic is further configured to:

encrypt the data block;

store the encrypted data block, the second data string, and the third data string;

access the encrypted data block, the second data string, and the third data string from storage; ~~and~~

obtain a signed second data string from the second device;

regenerate the encryption key from the signed second data string and the third data string; and

decrypt the encrypted data block using the regenerated encryption key.

74. (Currently amended) The ~~arrangement~~ system as recited in Claim 73, wherein the resulting decrypted data block includes ~~a~~ the first data string.

75. (Currently amended) The ~~arrangement~~ system as recited in Claim 74, wherein the resulting decrypted data block includes a hash of the first data string, and the first logic verifies the regenerated encryption key by hashing the first data string from the decrypted data block and comparing the hash of the decrypted first data string with the hash of the first data string obtained from the decrypted data block.

76. (Currently amended) The ~~arrangement~~ system as recited in Claim 73, further comprising memory operatively coupled to the first logic, and wherein the first logic reads the plurality of stored data strings and the encrypted data block from the memory.

77. (Currently amended) The ~~arrangement~~ system as recited in Claim 73, further comprising a data storage device having at least one storage medium, and wherein the first logic reads the plurality of stored data strings and the encrypted data block from the storage medium.

78. (Canceled)

79. (Currently amended) The ~~arrangement~~ system as recited in Claim ~~78~~ 72, wherein the first logic is further configured to generate the encryption key by cryptographically hashing the digitally signed second data string concatenated with the third data string.

80. (Currently amended) The ~~arrangement~~ system as recited in Claim ~~78~~ 72, wherein the first logic is further configured to generate the encryption key by cryptographically hashing the third data string concatenated with the digitally signed second data string.

81. (Currently amended) The ~~arrangement~~ system as recited in Claim 72, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a ~~substantially~~ randomly generated data string.

82. (Canceled)